REMARKS

This Application has been carefully reviewed in light of the Office Action mailed February 7, 2007. Claims 1-41 were pending in the Application. In the Office Action, Claims 1-41 were rejected. Claim 34 was objected to for informalities. In order to expedite prosecution of this Application, Applicants amends Claim 34. Thus, Claims 1-41 remain pending in the Application. Applicants respectfully request reconsideration and favorable action in this case.

In the Office Action, the following actions were taken or matters were raised:

CLAIM OBJECTIONS

The Examiner objected to Claim 34. Specifically, the Examiner states that the term "security model" should be changed to "security module". Applicants have amended Claim 34 accordingly. Applicants respectfully submit that the amendment to Claim 34 is to correct a typographical error, is not based on any cited reference and, therefore, does not narrow or otherwise change the scope of Claim 34. Therefore, Applicants respectfully request that this rejection be withdrawn.

SECTION 103 REJECTIONS

Claims 1-24 and 37-41 were rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Publication No. 2005/0044386 issued to *Libin* et al. (hereinafter "*Libin*") in view of U.S. Patent Publication No. 2003/0226036 issued to *Bivens* et al. (hereinafter "*Bivens*"). Claims 25-36 was rejected under 35 U.S.C. §103(a) as being unpatentable over *Libin*. Applicants respectfully traverse these rejections.

Of the rejected claims, Claims 1, 11, 16, 25, 31, and 37 are independent. Applicants respectfully submit that independent Claims 1, 11, 16, 31, and 37 are patentable over *Libin* in view of *Bivens*, and Claim 25 is patentable over *Libin*. Independent Claim 1 recites "[a] computer security system, comprising: a self-managed device having an authentication system for controlling access to the self-managed device by a user; and a security module adapted to authenticate an identity of the user and, in response to user authentication, automatically generate, transparently to the user, device credential data verifiable by the authentication system to enable user access to the self-managed device" (emphasis added). Applicants submit that *Libin* does not teach or suggest the features asserted by the Examiner in the Office Action dated February 7, 2007. For example, *Libin* appears to disclose a validation unit 42 (e.g., the device which the examiner indicates as disclosing the feature of "an authentication system for controlling access to the self-managed device by a user" of Claim 1) disposed within an electronic device 24 of *Libin* which uses the credential data to grant what appears to be continued access or operability of electronic device 24 (e.g., the device which the examiner indicates as disclosing the feature of a "self-managed device" of Claim 1). (*See* Office Action dated February 7, 2007, page 2). Paragraph 11 of *Libin* states that the "credentials/proofs may include a password entered by a user" and may also "include user biometric information." (*See* Office Action dated February 7, 2007, page 3). Thus, in order to receive the credential data from the user, the user would have already accessed electronic device 24 to provide the password or biometric information thereto. In contrast, Claim 1 recites a "security module adapted to authenticate an identity of [a] user, and, in response to user authentication, automatically generate,...device credential data verifiable by the authentication system to enable user access to the self-managed device." Thus, for at least this reason, *Libin* does not disclose or even suggest the limitation of Claim 1. Moreover, *Bivens* does not appear to remedy, nor did the Examiner rely on *Bivens* to remedy, at least this deficiency in *Libin*.

Furthermore, *Libin* does not disclose or even suggest a "security module adapted to authenticate an identify of the user and...automatically generate...device credential data verifiable by the authentication system to enable user access to the self-managed device" as recited by Claim 1. Validation unit 42 of *Libin* only appears to use the generated credential data and does not "automatically generate...device credential data". (See *Libin*, page 8, paragraph 45). Therefore, validation device 42 does not disclose all the features of the "security module" as recited in Claim 1. Additionally, administrative entity 28 of *Libin* appears to generate credential data but does not authenticate an user. For example, in paragraph 59 of *Libin*, the validation unit 42 determines if the "other information", which includes the identification of the user, is okay as part of the process of validating credentials for a user. (See page 10). Although the credentials may include the identify of the user, according to *Libin*, the validation unit 42 actually authenticates the user. Therefore, for at least these reasons, *Libin* does not disclose or even suggest the limitations of Claim 1. Furthermore, *Bivens* does not appear to remedy, nor did the Examiner rely on *Bivens* to remedy, at least this deficiency in *Libin*.

Moreover, the Examiner admits in the Office Action, and Applicants agree, that *Libin* does not disclose the described feature of generating credential data "transparently to the user" as recited in Claim 1. (*See* Office Action dated February 17, 2007, page 3). Further, contrary to the Office Action's assertion, Applicants do not agree that it would have been obvious to "interpret that the credentials were generated transparent to the user because the reference does not state that the credentials are made available to the user" (Office Action dated February 17, 2007, pg. 3). First, just because something is absent or omitted from a reference does not automatically imply that the feature exists or is present in the reference. To make such an assertion, the Office Action implies that the feature is "inherently present". But, to be "inherently present", the feature must "be necessarily present" and arise from the nature of the invention or be a natural outcome of the invention. Such a situation does not apply in this context. The fact that the credentials in *Libin* are "created and stored" does not automatically lead to the conclusion that credentials are "automatically generated, transparently to the user" as recited in Claim 1.

Second, *Libin* appears to disclose that users are prompted for a proof when validating the credentials in *Libin*. *Libin* specifically states:

> [0052] If it is determined at the test step 98 that an appropriate proof is not available externally, either because there is no appropriate connection or for some other reason, then control transfers from the test step 98 to a step 102 where the user is prompted to enter an appropriate proof. In an embodiment herein, if a user is at a location without an appropriate electrical connection, the user may call a particular phone number and receive an appropriate proof in the form of a number that may be entered manually into the electronic device in connection with the prompt provided at the step 102. Of course, the user may receive the proof by other means, such as being handwritten or typed or even published in a newspaper (e.g., in the classified section). *Libin*, page 9, paragraph 52 (emphasis added).

Thus, if a user is prompted as indicated in *Libin*, then the generation of device credential data cannot be transparent to the user. Thus, *Libin* appears to teach away from the limitations of Claim 1. Thus, for at least these reasons also, Claim 1 is patentable over the cited reference.

Moreover, the Office Action admits, and the Applicants agree, that *Libin* does not disclose the feature of "in response to user authentication, automatically generate...device credential data verifiable by the authentication system to enable user access to the self-managed device" as recited by Claim 1 (emphasis added). *Libin* appears to generate credentials independently of a user authentication, and *Libin* appears to perform the two actions in reverse. *Libin* appears to use and process the user identification information after processing the credentials, as shown in blocks 154 and 156 of the flowchart illustrated in Figure 6 of *Libin*. The text emphasizing that point is presented as follows:

> [0058] Referring to FIG. 6, a flow chart 150 illustrates steps performed by the validation unit 42 in connection with determining the validity of a proof. Processing begins at a first step 152 where the validation unit 42 receives the proof (e.g., by reading the proof from the proof data 44). Following the step 152 is a step 154 where the validation unit 42 receives the credentials (e.g., by reading the credential data 46).
>
> [0059] Following step 154 is a test step 156 which determines if the other information that is provided with the credentials is okay. As discussed elsewhere herein, the other information includes, for example, an identification of the electronic device, an identification of the user, or other property identifying information. If it is determined at the test step 156 that the other information associated with the credentials does not match the particular property described by the other information (e.g., the credentials are for a different electronic device or different user), then control transfers from the test step 156 to a step 158 where a fail signal is provided. Following the step 158, processing is complete. *Libin*, page 10, paragraphs 58-59 (emphasis added).

Therefore, *Libin* does not teach or suggest the feature of "in response to user authentication, automatically generate...device credential data verifiable by the authentication system to enable user access to the self-managed device" as recited in Claim 1. Accordingly, Claim 1 is patentable over *Libin*. Accordingly, for these reasons, Applicants respectfully submit that Claim 1 is patentable over *Libin* in view of *Bivens*.

The cited references also do not teach or suggest the features of Claim 25. Independent claim 25 recites "an activation/deactivation module accessible via a networked administration client, the activation/deactivation module adapted to interface with the security module in response to a request by the administration client to activate, transparently to the user, an authentication system of a self-managed device to control user access to the self-managed device" (emphasis added). As shown above, *Libin* does not teach or suggest, expressly or implicitly, the feature of "transparently to the user", and, as shown above, *Libin* teaches away from the feature. Therefore, at least for this reason, Claim 25 is patentable over *Libin*.

Furthermore, *Libin* does not disclose the feature of "an activation/deactivation module accessible via a networked administration client, the activation/deactivation module adapted to interface with the security module in response to a request by the administration client to activate...an authentication system of a self-managed device to control user access to the self-managed device." The Office Action asserts that the feature is disclosed in *Libin* because a "second entity working for administrative entity" "causes the validation unit to examine credential data". (Office Action dated February 7, 2007, page 11). However, the Office Action misconstrues the cited sections of text. First, in *Libin*, the "second entity working for administrative entity" does not "cause the validation unit to examine credential data". In paragraph 45 of the reference, a "start signal...causes the validation unit 42 to examine the credential data 44 and the proof data 46". (*Libin*). The start signal is transmitted at "boot up", which is a function not caused by the second entity described in *Libin*. (See paragraph 38 and 45). The second entity, as reference in *Libin*, manages a smart door access system. (See paragraph 67). The smart door access system is a "physical access" that specifies to which door a user has access. The second entity manages the authentication. Nowhere does *Libin* appear to indicate that the second entity causes the examination of credential data in the validation unit. Furthermore, nowhere in *Libin* does there appear to be any indication that the second entity manages the "boot up" which causes the validation unit to examine credential data. Moreover, nowhere in *Libin* does there appear to be any indication that the second entity is a "networked administration client" as recited in Claim 25. Therefore, *Libin* does not teach or suggest all the features of Claim 25. Accordingly, Applicants submits that Claim 25 is patentable over *Libin*.

Since independent Claims 11, 16, 25, 31, and 37 include similar features as claim 1, the arguments presented above also apply to Claims 11, 16, 25, 31, and 37. Therefore, Claims 11, 16, 25, 31, and 31 are also patentable over *Libin* in view of *Bivens*. Furthermore, Claims 2-10, 12-15, 17-24, 26-30, 32-36, and 28-41 depend from Claims 1, 11, 16, 25, 31, and 37, respectfully, and also, therefore are patentable over *Libin* in view of *Bivens*.

CONCLUSION

Applicants has made an earnest attempt to place this case in condition for immediate allowance. For the foregoing reasons and for other reasons clearly apparent, Applicants respectfully requests reconsideration and full allowance of all pending claims.

No fee is believed due with this Response. If, however, Applicants has overlooked the need for any fee due with this Response, the Commissioner is hereby authorized to charge any fees or credit any overpayment associated with this Response to Deposit Account No. 08-2025 of Hewlett-Packard Company.

Respectfully submitted,

By: Hope Shimabuku
Hope Shimabuku
Reg. No. 57,072

Date: 5/7/07

Correspondence to:

Hewlett-Packard Company
Intellectual Property Administration
P. O. Box 272400
Fort Collins, CO 80527-2400
Tel. 970-898-3884